PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of	:	Petrus Lambertus Adrianus Roelse
For	:	LINEAR TRANSFORMATION FOR SYMMETRIC-KEY CIPHERS
Serial No.:	:	09/918,831
Filed	:	August 1, 2001
Art Unit	:	2137
Examiner	:	Michael J. Pyzocha
Att. Docket	:	NL-000444
Confirmation No.	:	4772

APPEAL BRIEF

Mail Stop Appeal Brief Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed November 13, 2006, further to the Appeal Brief filed January 17, 2007, and in response to the Notice Under 37 C.F.R. 41.37 mailed April 13, 2007.

I. REAL PARTY IN INTEREST

The party in interest is the assignee, Koninklijke Philips Electronics, N.V. The assignment document is recorded at Reel 012497 and Frame 0850.

II. RELATED APPEALS AND INTERFERENCES

Following are identified any prior or pending appeals, interferences or judicial proceedings, known to Appellant, Appellant's representative, or the Assignee, that may be related to, or which will directly affect or be directly affected by or have a bearing upon the Board's decision in the pending appeal:

NONE.

III. STATUS OF CLAIMS

This is an appeal from the Final Office Action dated September 12, 2006, rejecting claims 1, 2, 6-8, 11 and 15. The claims being appealed are claims 1, 2, 6-8, 11 and 15. Claims 9 and 10 have been cancelled. The Office Action allowed claim 16 and indicated that claims 3-5 and 12-14 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Claims 1-8 and 11-16 are all the pending claims.

IV. STATUS OF AMENDMENTS

All Amendments have been entered into the record.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 relates to a method of linear transformation in a symmetric-key cipher comprising inputting block data into a processing apparatus; creating a linear

transformation matrix A with the processing apparatus by: generating a binary [n,k,d] error-correcting code, represented by a generator matrix $G \in Z_2^{k \times n}$ in a form $G = (I_k \| B)$, with $B \in Z_2^{k \times (n-k)}$, where $k < n < 2k$, and d is the minimum distance of the binary error-correcting code; shortening said error-correcting code; and extending matrix B with 2k-n columns such that a resulting matrix C is non-singular, and deriving the linear transformation matrix A from matrix C; and transforming the input block data into diffused output block data with the processing apparatus by using the linear transformation matrix A. *See*, page 3, line 20 to page 11, line 14.

Independent claim 8 relates to a system for cryptographically converting an input data block into an output data block, the input data blocks comprising n data bits, the system comprising: an input for receiving the input data block; a storage for storing a linear transformation matrix A created by: generating a binary [n,k,d] error-correcting code, represented by a generator matrix $G \in Z_2^{k \times n}$ in a form $G = (I_k \| B)$, with $B \in Z_2^{k \times (n-k)}$, where $k < n < 2k$, and d is the minimum distance of the binary error-correcting code; shortening said error-correcting code; and extending matrix B with 2k-n columns such that a resulting matrix C is non-singular, and deriving the linear transformation matrix A from matrix C; a cryptographic processor performing a linear transformation on the input data block or a derivative of the input data block using the linear transformation matrix A; and an output for outputting the processed input data block. *See*, page 3, line 28 to page 7, line 21.

Independent claim 16 relates to a method of linear transformation in a symmetric-key cipher comprising: inputting block data into a processing apparatus; creating a linear

transformation matrix A with the processing apparatus by: generating a binary [n,k,d] error-correcting code, represented by a generator matrix $G \in Z_2^{k \times n}$ in a form $G = (I_k \| B)$, with $B \in Z_2^{k \times (n-k)}$, where $k < n < 2k$, and d is the minimum distance of the binary error-correcting code; extending matrix B with 2k-n columns such that a resulting matrix C is non-singular; determining two permutation matrices $P_1, P_2 \in Z_2^{k \times k}$ such that all codewords in an [2k,k,d] error-correcting code, represented by the generator matrix $(I_k \| P_1 C P_2)$, have a predetermined multi-bit weight; and using $P_1 C P_2$ as matrix A; and transforming the input block data into diffused output block data with the processing apparatus by using the linear transformation matrix A. *See*, page 3, line 20 to page 11, line 14.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following grounds of rejection are presented for review:

A. Claims 1, 7 and 8 were rejected under 35 U.S.C. § 103(a) as being allegedly obvious over Rijmen et al. (hereinafter noted "Rijmen") in view of Loureiro et al. (hereinafter noted "Loureiro") and further in view of Knudsen et al. (hereinafter noted "Knudsen").

B. Claims 2 and 11 were rejected under 35 U.S.C. § 103(a) as being allegedly obvious over Rijmen/Loureiro/Knudsen and further in view of a FOLDOC article on "brute force" (hereinafter noted "FOLDOC").

C. Claims 6 and 15 were rejected under 35 U.S.C. § 103(a) as being allegedly obvious over Rijmen/Loureiro/Knudsen and further in view of Isaka et al. (hereinafter noted "Isaka").

VII. ARGUMENT

All of the rejections are rejections under 35 U.S.C. § 103(a). The test for determining if a claim is rendered obvious by one or more references for purposes of a rejection under 35 U.S.C. § 103 is set forth in MPEP § 706.02(j), based on the cited authority of the Court of Appeals for the Federal Circuit:

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Therefore, if the above-identified criteria are not met, then the cited reference(s) fails to render obvious the claimed invention and, thus, the claimed invention is distinguishable over the cited references.

A. Rejection of Claims 1, 7 and 8 Under 35 U.S.C. §103(a)

The Final Office Action dated September 12, 2006, rejects claims 1, 7 and 8 under 35 U.S.C. § 103(a) as being allegedly obvious over Rijmen in view of Loureiro and further in view of Knudsen.

1. Claims 1 and 8

Claims 1 and 8 are directed, respectively, to a method and a system for linear transformation

in a symmetric-key cipher. The method comprises: generating a binary error-correcting code, represented by a generator matrix G in a form $G = (I_k \| B)$; and extending matrix B with 2k-n columns such that a resulting matrix C is non-singular, and deriving the linear transformation matrix A from matrix C.

In rejecting claims 1 and 8 (and 7), the Office Action relies on the combination of three references. As correctly conceded by the Office Action, Rijmen does not disclose, teach or suggest extending matrix B and deriving matrix A from matrix C, as recited in claims 1 and 8. In order to overcome this correctly admitted deficiency in Rijmen, the Office Action relies upon reference, Loureiro. Appellant respectfully asserts that the Office correctly did not rely on Knudsen with respect to this subject matter for the reason that Knudsen also does not disclose, teach or suggest extending matrix B and deriving matrix A from matrix C, as recited in claims 1 and 8.

In asserting a motivation to combine the respective teachings of Rijmen and Loureiro (and Knudsen), to the exclusion of other respective teachings in Rijmen and Loureiro (and Knudsen), in the fourth full paragraph on page 3, the Office Action alleges a motivation for the combination. However, the motivation alleged by the Office Action stands alone and unsupported in any way. No basis or support for the alleged motivation is put forth by the Office Action in any way.

It is impermissible for an Examiner to engage in hindsight reconstruction of the prior art using Applicant's claims as a template and selecting elements from references to fill the page.

Rather, prior art references may be modified or combined to render obvious a subsequent invention only if there was some suggestion or motivation to do so derived from the prior art itself, the nature of the problem to be solved, or the knowledge of one of ordinary skill in the art. *Sibia Neurosciences*, 225 F.3d 1349, 1356 (Fed. Cir. 2000); *ATD Corp. v. Lydall, Inc.*, 159 F.3d 534, 546 (Fed. Cir. 1998).

In order to be directed to unpatentable (i.e., obvious) subject matter, one of two things must be true. Either (1) the references must expressly suggest the claimed combination or imply the same, or (2) the Examiner must present a convincing line of reasoning as to why the applicable artisan would have found the claimed invention to have been obvious in the light of the teachings of the references. The motivation to make a specific structure is not abstract, but practical, and is always related to the properties or uses one skilled in the art would expect the structure to have, if made. The critical inquiry is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making that structure. *See In re Newell*, 13 USPQ2d 1248, 1250 (Fed. Cir. 1989).

The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *See In re Mills*, 916 F.2d 680, 16 USPQ2d 1430, 1432 (Fed. Cir. 1990) (holding that, although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so"); *see also In re Fritch*, 972 F.2d 1260, 23 USPQ2d 1780 (Fed. Cir. 1992). Similarly, even if the references relied upon establish that all

aspects of the claimed invention were individually known in the art at the time the claimed invention was made, a statement by the Examiner that modifications of the prior art to meet the claimed invention would have been within the ordinary skill of the art is not sufficient to establish a prima facie case of obviousness without some objective reason to combine the teachings of the references. *See Ex parte Levengood*, 28 USPQ2d 1300 (Bd. Pat. App. & Inter. 1993).

Thus, obviousness is tested by "what the combined teachings of the references would have suggested to those of ordinary skill in the art." *In re Keller*, 642 F.2d 413, 425, 208 USPQ 871, 881 (CCPA 1981). However, the obviousness of the claimed invention "cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination." *ACS Hosp. Sys.*, 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). Thus, "teachings of references can be combined only if there is some suggestion or incentive to do so." *Id.*

Most if not all inventions arise from a combination of old elements. *In re Kotzab*, 55 USPQ2d 1313, 1316 (Fed. Cir. 2000) (citing *In re Rouffet*, 149 F.3d 1350, 1357, 47 USPQ2d 1453, 1457 (Fed. Cir. 1998)). Thus, every element of a claimed invention may often be found in the prior art. *Id.* However, identification in the prior art of each individual part claimed is insufficient to defeat patentability of the whole claimed invention. *Id.* Rather, to establish obviousness based on a combination of the elements disclosed in the prior art, there must be some motivation, suggestion or teaching of the desirability of making the specific combination

claimed by the applicant. *See In re Sang Su*, 277 F.3d 1338, 61 USPQ2d 1430 (Fed. Cir. 2002); *In re Kotzab*, 55 USPQ2d at 1316 (citing *In re Dance*, 160 F.3d 1339, 1343, 48 USPQ2d 1635, 1637 (Fed. Cir. 1998)); *In re Gordon*, 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984)). Further, "when the PTO asserts that there is an explicit or implicit teaching or suggestion in the prior art, it must indicate where such a teaching or suggestion appears in the reference." *In re Rijckaert*, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993) (citing *In re Yates*, 663 F.2d 1054, 211 USPQ 1149, 1151 (CCPA 1981)). Here, the rejection makes no indication of where the alleged motivation is coming from, not by indicating support for the alleged motivation in the applied references, and not by making any other statement of a basis for the alleged motivation.

"'The factual inquiry whether to combine references must be thorough and searching.'" *In re Sang Su*, 277 F.3d 1338, 61 USPQ2d 1430 (Fed. Cir. 2002) (quoting *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339, 1351-52, 60 USPQ2d 1001, 1008 (Fed. Cir. 2001)). Here, the Examiner has not conducted the requisite "thorough and searching" factual inquiry. Rather, the Examiner has made no indication whatsoever of where a teaching or suggestion appears in the prior art references that they be combined in the manner necessary to result in the claimed invention. The Examiner has not alleged that the motivation to combine the references as necessary arrives from the nature of the problem to be solved, or from anywhere else. The "factual question of motivation [to combine references] is material to patentability, and [can] not be resolved on subjective belief and unknown authority." *In re Sang Su*, 277 F.3d 1338, 61 USPQ2d 1430 (Fed. Cir. 2002).

Here, it appears that the Examiner improperly relies on "subjective belief and unknown authority" to establish the motivation to combine references essential to an obviousness inquiry, because the Examiner has provided no citation within the references themselves, and has failed to even allege any basis for the alleged motivation. The Examiner certainly has not provided factual basis that the claimed subject matter would have been obvious to a person having an ordinary level of skill in the art at the time the invention was made. In fact, the Examiner hasn't even made that allegation.

"Although the suggestion to combine references may flow from the nature of the problem, 'defining the problem in terms of its solution reveals improper hindsight in the selection of the prior art relevant to obviousness.'" *Exolochem, Inc. v. Southern Cal. Edison Co.*, 2000 U.S. App. LEXIS 22681, *28 (Fed. Cir. 2000) (citing *Monarch Knitting Mach. Corp. v. Sulzer Morat Gmbh*, 139 F.3d 877, 880, 45 USPQ2d 1977, 1981 (Fed. Cir. 1998)). Thus, "[i]t is improper, in determining whether a person of ordinary skill would have been led to this combination of references, simply to '[use] that which the inventor taught against its teacher.'" *In re Sang Su*, 277 F.3d 1338, 61 USPQ2d 1430 (Fed. Cir. 2002) (quoting *W.L. Gore v. Garlock, Inc.*, 721 F.2d 1540, 1553, 220 USPQ 303, 312-13 (Fed. Cir. 1983)). "Therefore, when determining the patentability of a claimed invention which combines two known elements, the question is whether there is something in the prior art as a whole to suggest the desirability, and thus obviousness, of making the combination." *Id.* at *29-30 (citing *In re Beattie*, 974 F.2d 1309, 1311-12, 24 USPQ2d 1040, 1042 (Fed. Cir. 1992)).

Although a reference need not expressly teach that the disclosure contained therein should be combined with another, the showing of combining the two, in whatever form, must nevertheless be "clear and particular. *Winner Int'l Royalty Corp. v. Ching-Rong Wang*, 202 F.3d 1340, 1348-49, 53 USPQ2d 1580, 1586-87 (Fed. Cir. 2000) (citations omitted).

Here, the prior art contains no such "clear and particular" expression of the desirability of combining the particular teachings contained therein so as to arrive at the claimed combination. Instead, the Examiner relies on impermissible hindsight in reaching a determination of obviousness, defining the problem in terms of its solution.

A critical step in analyzing the patentability of claims pursuant to section 103(a) is casting the mind back to the time of invention, to consider the thinking of one of ordinary skill in the art, guided only by the prior art references and the then-accepted wisdom in the field. *See In re Kotzab*, 55 USPQ2d 1313, 1316 (Fed. Cir. 2000) (citing *In re Dembiczak*, 175 F.3d 994, 999, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999)). Close adherence to this methodology is especially important in cases where the very ease with which the invention can be understood may prompt one "to fall victim to the insidious effect of a hindsight syndrome wherein that which only the invention taught is used against its teacher." *Kotzab*, 55 USPQ2d at 1316 (quoting *W.L. Gore & Assocs., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1553, 220 USPQ 303, 313 (Fed. Cir. 1983) ("[t]o imbue one of ordinary skill in the art with knowledge of the invention in suit, when no prior art reference or references of record convey or suggest that knowledge, is to fall victim to the

insidious effect of a hindsight syndrome wherein that which only the inventor taught is used against its teacher")).

It is well settled that "it is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position to the exclusion of other parts necessary to a full appreciation of what such reference fairly suggests to one skilled in the art." *See Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve*, 796 F.2d 443, 448, 230 USPQ. 416, 419 (Fed. Cir. 1986) (citing *In re Wesslau*, 353 F.2d 238, 241, 147 USPQ 391, 193 (CCPA 1965), cert. denied, 484 U.S. 823 (1987)). Here, this appears to be exactly what the Examiner has done.

When the only suggestion of a claimed feature on the record is that of the pending application, a rejection under § 103 is improper. *See In re Laskowski*, 10 USPQ2d 1397 (Fed. Cir. 1989). Here, that appears to be the case.

Applicant respectfully asserts that only by the impermissible use of hindsight knowledge of Applicant's own disclosure would the Examiner have acquired a motivation to combine the teachings of the three cited references according the precise combination including certain elements and excluding certain others as necessary to achieve the subject matter according to the combinations recited in independent claims 1 and 8.

For at least the foregoing reasons, claims 1 and 8 are patentable over Rijmen and Loureiro and Knudsen because, in asserting a motivation to combine the respective teachings of the three

references, to the exclusion of other respective teachings in Rijmen and Loureiro and Knudsen, in the fourth full paragraph on page 3, the Office Action fails to state any basis for the alleged motivation for the combination put forth.

In section 7 on pages 6-8, the Office Action includes a section entitled, "Response to Arguments." The section specifically responds to the above argument in the second paragraph on page 6. Specifically, the Office Action refers to section 4, titled Function Hiding, of the Loureiro reference in support of the alleged motivation to combine.

However, an object of the subject matter recited in the rejected claims is to provide an invertible linear transformation, represented by a non-singular binary matrix, for use in symmetric-key ciphers with guaranteed optimal diffusion characteristics on a bit-level based on an optimal binary linear error-correcting code. This transformation is advantageous in that it is more irregular, and this avoids additional mathematical structure of the resulting linear transformation which could be exploited in cryptanalysis. *See*, application page 2, lines 22-27. In contrast, the function hiding described in section 4 of Loureiro does not pertain to the object of the subject matter recited in the rejected claims as described above.

2. Claims 3-5, 7 and 12-14

Claim 7 depends from claim 1 and is therefore also patentable for at least the reasons stated above in connection with claim 1, as well as for the separately patentable subject matter recited therein. Claims 3-5 and 12-14 depend from claims 1 and 8, respectively. This being the only rejection of claims 1 and 8, claims 3-5 and 12-14 are also patentable for at least the reasons stated

above in connection with claims 1 and 8, as well as for the separately patentable subject matter recited therein. This assertion has been admitted by the Examiner with respect to claims 3-5 and 12-14 (objected to).

B. Rejection of Claims 2 and 11 Under 35 U.S.C. §103(a)

The Final Office Action dated September 12, 2006, rejects claims 2 and 11 under 35 U.S.C. § 103(a) as being allegedly obvious over Rijmen/Loureiro/Knudsen and further in view of FOLDOC.

This rejection relies on a combination of four references. Thus, the deficiencies describe above in connection with claims 1 and 8, from which claims 2 and 11 depend, respectively, in the asserted motivation to combine the three references applied in rejecting claims 1 and 8 are further exacerbated by the additional reliance on FOLDOC in further combination with Rijmen in view of Loureiro and further in view of Knudsen.

For at least the foregoing reasons, claims 2 and 11 are patentable over Rijmen in view of Loureiro, further in view of Knudsen, and still further in view of FOLDOC, because a motivation has not properly been established to combine the respective teachings of Rijmen in view of Loureiro, further in view of Knudsen, and still further in view of FOLDOC, to the exclusion of the other teachings in Rijmen in view of Loureiro, further in view of Knudsen, and still further in view of FOLDOC, in order to arrive at the precise combinations recited in claims 2 and 11.

C. Rejection of Claims 6 and 15 Under 35 U.S.C. §103(a)

The Final Office Action dated September 12, 2006, rejects claims 6 and 15 under 35 U.S.C. § 103(a) as being allegedly obvious over Rijmen/Loureiro/Knudsen and further in view of Isaka.

This rejection relies on a combination of four references. Thus, the deficiencies describe above in connection with claims 1 and 8, from which claims 6 and 15 depend, respectively, in the asserted motivation to combine the three references applied in rejecting claims 1 and 8 are further exacerbated by the additional reliance on Isaka in further combination with Rijmen in view of Loureiro and further in view of Knudsen.

For at least the foregoing reasons, claims 6 and 15 are patentable over Rijmen in view of Loureiro, further in view of Knudsen, and still further in view of Isaka, because a motivation has not properly been established to combine the respective teachings of Rijmen in view of Loureiro, further in view of Knudsen, and still further in view of Isaka, to the exclusion of the other teachings in Rijmen in view of Loureiro, further in view of Knudsen, and still further in view of Isaka, in order to arrive at the precise combinations recited in claims 6 and 15.

CONCLUSION

For at least the reasons discussed above, it is respectfully submitted that the rejections are in error and that claims 1-8 and 11-16 are all in condition for allowance. For at least the above reasons, Appellants respectfully request that this Honorable Board reverse the rejections of claims 1, 2, 6-8, 11 and 15.

Respectfully submitted,
KRAMER & AMADO, P.C.

May 14, 2007
Date: May 14, 2007

Mark R. Woodall
Reg. No. 43,286

KRAMER & AMADO, P.C.
1725 Duke Street, Suite 240
Alexandria, VA 22314
Tel. (703) 519-9801
Fax. (703) 519-9802

DIRECT ALL CORRESPONDENCE TO:
Eric Bram, Registration No. 37,285
US PHILIPS CORPORATION
P.O. Box 3001
Briarcliff Manor, NY 10510-8001
Phone: (914) 333-9635
Fax: (914) 332-0615

VIII. CLAIMS APPENDIX

CLAIMS INVOLVED IN THE APPEAL:

1. A method of linear transformation in a symmetric-key cipher comprising:

inputting block data into a processing apparatus;

creating a linear transformation matrix A with the processing apparatus by:

generating a binary [n,k,d] error-correcting code, represented by a generator matrix $G \in Z_2^{k \times n}$ in a form $G = (I_k \| B)$, with $B \in Z_2^{k \times (n-k)}$, where $k < n < 2k$, and d is the minimum distance of the binary error-correcting code;

shortening said error-correcting code; and

extending matrix B with 2k-n columns such that a resulting matrix C is non-singular, and deriving the linear transformation matrix A from matrix C; and

transforming the input block data into diffused output block data with the processing apparatus by using the linear transformation matrix A.

2. A method as claimed in claim 1, wherein extending matrix B with 2k-n columns comprises:

in an iterative manner:

randomly generating 2k-n columns, each with k binary elements;

forming a test matrix consisting of the n-k columns of B and the 2k-n generated columns; and

checking whether the test matrix is non-singular, until a non-singular test matrix has been found; and

using the found test matrix as matrix C.

3. A method as claimed in claim 1, wherein the operation of deriving matrix A from matrix C comprises:

determining two permutation matrices $P_1, P_2 \in Z_2^{k \times k}$ such that all codewords in an [2k,k,d] error-correcting code, represented by the generator matrix $(I_k \parallel P_1 C P_2)$, have a predetermined multi-bit weight; and

using $P_1 C P_2$ as matrix A.

4. A method as claimed in claim 3, wherein the input block data is m-bit sub-block data, and the processing apparatus executes a round function with an S-box layer with S-boxes operating on the m-bit sub-blocks data, and the minimum predetermined multi-bit weight over all non-zero codewords equals a predetermined m-bit weight.

5. A method as claimed in claim 3, wherein determining the two permutation matrices P_1 and P_2 comprises iteratively generating the matrices in a random manner.

6. A method as claimed in claim 1, wherein the input block data is 32-bit block data and

wherein the operation of generating a [n,k,d] error-correcting code comprises:

generating a binary extended Bose-Chaudhuri-Hocquenghem (XBCH) [64,36,12] code; and

shortening the XBCH [64,36,12] code to a [60,32,12] XBCH code by deleting four rows.

7. A computer program product stored on a computer readable medium, wherein the program product is operative to cause the a processor to perform the method of claim 1.

8. A system for cryptographically converting an input data block into an output data block, the input data blocks comprising n data bits, the system comprising:

an input for receiving the input data block;

a storage for storing a linear transformation matrix A created by:

generating a binary [n,k,d] error-correcting code, represented by a generator matrix $G \in Z_2^{k \times n}$ in a form $G = (I_k \| B)$, with $B \in Z_2^{k \times (n-k)}$, where $k < n < 2k$, and d is the minimum distance of the binary error-correcting code;

shortening said error-correcting code; and

extending matrix B with 2k-n columns such that a resulting matrix C is non-singular, and deriving the linear transformation matrix A from matrix C;

a cryptographic processor performing a linear transformation on the input data block or a derivative of the input data block using the linear transformation matrix A; and

an output for outputting the processed input data block.

11. A system as claimed in claim 8, wherein extending matrix B with 2k-n columns comprises:

in an iterative manner:

randomly generating 2k-n columns, each with k binary elements;

forming a test matrix consisting of the n-k columns of B and the 2k-n generated columns; and

checking whether the test matrix is non-singular, until a non-singular test matrix has been found; and

using the found test matrix as matrix C.

12. A system as claimed in claim 8, wherein the operation of deriving matrix A from matrix C comprises:

determining two permutation matrices $P_1, P_2 \in Z_2^{k \times k}$ such that all codewords in an [2k,k,d] error-correcting code, represented by the generator matrix $(I_k \| P_1 \, C \, P_2)$, have a predetermined multi-bit weight; and

using $P_1 \, C \, P_2$ as the matrix A.

13. A system as claimed in claim 12, wherein the input block data is m-bit sub-block data,

and the processing apparatus executes a round function with an S-box layer with S-boxes operating on the m-bit sub-block data, and the minimum predetermined multi-bit weight over all non-zero codewords equals a predetermined m-bit weight.

14. A system as claimed in claim 12, wherein determining the two permutation matrices P_1 and P_2 comprises iteratively generating the matrices in a random manner.

15. A system as claimed in claim 8, wherein the input data block is a 32-bit data block and wherein the operation of generating a [n,k,d] error-correcting code comprises:

generating a binary extended Bose-Chaudhuri-Hocquenghem (XBCH) [64,36,12] code; and

shortening the XBCH [64, 36, 12] code to a [60, 32, 12] XBCH code by deleting four rows.

16. A method of linear transformation in a symmetric-key cipher comprising:

inputting block data into a processing apparatus;

creating a linear transformation matrix A with the processing apparatus by:

generating a binary [n,k,d] error-correcting code, represented by a generator matrix $G \in Z_2^{k \times n}$ in a form $G = (I_k \| B)$, with $B \in Z_2^{k \times (n-k)}$, where $k < n < 2k$, and d is the minimum distance of the binary error-correcting code;

extending matrix B with 2k-n columns such that a resulting matrix C is non-singular;

determining two permutation matrices $P_1, P_2 \in Z_2^{k \times k}$ such that all codewords in an [2k,k,d] error-correcting code, represented by the generator matrix $(I_k \| P_1 C P_2)$, have a predetermined multi-bit weight; and

using $P_1 C P_2$ as matrix A; and

transforming the input block data into diffused output block data with the processing apparatus by using the linear transformation matrix A.

IX. EVIDENCE APPENDIX

A copy of the following evidence 1) entered by the Examiner, including a statement setting forth where in the record the evidence was entered by the Examiner, 2) relied upon by the Appellant in the appeal, and/or 3) relied upon by the Examiner as to the grounds of rejection to be reviewed on appeal, is attached:

NONE

X. RELATED PROCEEDINGS APPENDIX

Copies of relevant decisions in prior or pending appeals, interferences or judicial proceedings, known to Appellant, Appellant's representative, or the Assignee, that may be related to, or which will directly affect or be directly affected by or have a bearing upon the Board's decision in the pending appeal are attached:

NONE